(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-505873
(P2005-505873A)
(43)公表日　平成17年2月24日(2005.2.24)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 12/14	G06F	12/14	540A	5B017
G09C 1/00	G06F	12/14	540P	5D044
G11B 20/10	G09C	1/00	660D	5J104
	G11B	20/10	D	
	G11B	20/10	H	

審査請求 未請求　予備審査請求 未請求　（全 38 頁）　最終頁に続く

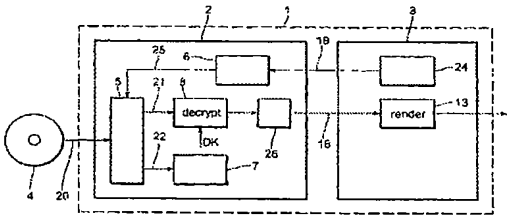
(21)出願番号　特願2003-537067 (P2003-537067)
(86)(22)出願日　平成14年9月12日 (2002.9.12)
(85)翻訳文提出日　平成16年1月28日 (2004.1.28)
(86)国際出願番号　PCT/IB2002/003786
(87)国際公開番号　WO2003/034425
(87)国際公開日　平成15年4月24日 (2003.4.24)
(31)優先権主張番号　01203907.9
(32)優先日　平成13年10月12日 (2001.10.12)
(33)優先権主張国　欧州特許庁 (EP)

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　５６２１　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　１
Ｇｒｏｅｎｅｗｏｕｄｓｅｗｅｇ　１，５６２１　ＢＡ　Ｅｉｎｄｈｏｖｅｎ，Ｔｈｅ　Ｎｅｔｈｅｒｌａｎｄｓ
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100114753
弁理士　宮崎　昭彦

最終頁に続く

(54)【発明の名称】ブロックとして記憶されるユーザデータを読み取る又は書き込む装置及び方法

(57)【要約】
本発明は、記憶部がブロックに分かれている記憶媒体（４）に暗号化された形式でブロックとして記憶されたユーザデータ（２１）を読み取る又は書き込む装置と、記憶媒体（４）に暗号化された形式でブロックとしてユーザデータ（２１）を書き込む装置（１）と、対応する方法とに関する。前記ユーザデータは、前記記憶媒体（４）に暗号化された形式で記憶されるので、前記装置は、前記記憶媒体に書き込む前に前記ユーザデータを暗号化するために暗号化鍵について、又は出力する前に前記読み取られたユーザデータを解読するための解読鍵について知らされる必要がある。従って、本発明によると、前記読み取る装置が、＊どのユーザデータが読み取られるべきかを指定するユーザデータ情報を含む読み取りコマンド（１９）を受信し、翻訳するコマンド・インターフェース（６）と、＊前記記憶媒体のブロックからユーザデータ及び関連した暗号化インジケータを読み取る読み取り手段であって、前記暗号化インジケータは、前記ユーザデータが暗号化されているか否かを示し、更に、もし前記暗号化インジケータが、前記ユーザデータが暗号



【特許請求の範囲】
【請求項１】
記憶部がブロックに分かれている記憶媒体にブロックとして記憶されたユーザデータを読み取る装置であって、
・どのユーザデータが読み取られるべきかを指定するユーザデータ情報を含む読み取りコマンドを受信し、翻訳するコマンド・インターフェースと、
・前記記憶媒体のブロックからユーザデータ及び関連した暗号化インジケータを読み取る読み取り手段であって、前記暗号化インジケータは、前記ユーザデータが暗号化されているか否かを示し、更に、もし前記暗号化インジケータが、前記ユーザデータが暗号化されていることを示すならば、前記ユーザデータを解読するために、どの鍵データを使用するかを指定する関連した鍵データ識別子を読み取るように構成された当該読み取り手段と、
・前記鍵データを使用して前記ユーザデータを解読する解読手段と、
・前記解読されたユーザデータを出力する出力手段と、
を有する装置。
【請求項２】
前記鍵データが、前記記憶媒体に暗号化された形式で記憶され、
前記読み取り手段が、前記ユーザデータを解読するために使用されるべき前記鍵データを読み取るように構成され、
前記解読手段が、更に前記暗号化された鍵データを解読するように構成される、
請求項１に記載の装置。
【請求項３】
前記読み取りコマンドが、出力する前に前記解読されたユーザデータを再暗号化するために、どの再暗号化鍵データを使用するかを指定する再暗号化鍵データ情報を含み、
前記装置が、更に、前記出力手段により出力する前に前記解読されたユーザデータを再暗号化する再暗号化手段を有する、
請求項１に記載の装置。
【請求項４】
前記鍵データ識別子が、前記鍵データ識別子により指定された前記鍵データの使用により暗号化されたユーザデータを記憶するブロックのヘッダ又はサブヘッダに記憶される、請求項１に記載の装置。
【請求項５】
前記鍵データ識別子は、前記ユーザデータが読み取られるべき前記ブロックの隣に、特にメインデータチャネルのサブチャネルに記憶される、請求項１に記載の装置。
【請求項６】
初期化ベクトルが、関連したユーザデータを記憶するブロックのヘッダ又はサブヘッダに暗号化された形式で記憶される、請求項１に記載の装置。
【請求項７】
前記鍵データ識別子が、更に、アクセスされる前記ブロックに記憶された前記ユーザデータに関連する付加的な情報、特に権利情報を指定し、前記付加的な情報が、前記記憶媒体上の鍵ロッカーに記憶される、請求項１に記載の装置。
【請求項８】
記憶部がブロックに分かれている記憶媒体にブロックとして記録されたユーザデータを読み取る方法であって、
・どのユーザデータが読み取られるべきかを指定するユーザデータ情報を含む読み取りコマンドを受信し、翻訳するコマンド・インターフェースのステップと、
・前記記憶媒体のブロックからユーザデータ及び関連した暗号化インジケータを読み取る読み取り手段のステップであって、前記暗号化インジケータは、前記ユーザデータが暗号化されているか否かを示し、更に、もし前記暗号化インジケータが、前記ユーザデータが暗号化されていることを示すならば、前記ユーザデータを解読するために、どの鍵データを使用するかを指定する関連した鍵データ識別子を読み取るように構成された当該読み取

り手段のステップと、
・前記鍵データを使用して前記ユーザデータを解読する解読手段のステップと、
・前記解読されたユーザデータを出力する出力手段のステップと、
を有する方法。
【請求項９】
記憶部がブロックに分かれている記憶媒体にブロックとしてユーザデータを書き込む装置であって、
・どのユーザデータが書き込まれるべきかを指定するユーザデータ情報と、前記ユーザデータが暗号化された形式で書き込まれるべきであるかどうかを示す関連した暗号化インジケータとを含む書き込みコマンドを受信し、翻訳するコマンド・インターフェースと、
・鍵データを使用して前記ユーザデータを暗号化する暗号化手段と、
・前記ユーザデータと、前記暗号化インジケータと、もし前記ユーザデータが暗号化されるならば、どの鍵データが前記ユーザデータを暗号化するために使用されるかを指定する鍵データ識別子とを書き込む書き込み手段と、
を有する装置。
【請求項１０】
前記書き込みコマンドが、前記ユーザデータを暗号化するために使用されるべき前記鍵データを含み、前記鍵データが、暗号化された形式で含まれ、
前記装置が、更に、前記暗号化された鍵データを解読する鍵解読手段を有する、
請求項９に記載の装置。
【請求項１１】
前記鍵データが、前記記憶媒体に暗号化された形式で記憶され、
前記書き込みコマンドが、前記鍵データを識別する鍵データ識別子を含み、前記鍵データは、前記記憶媒体から読み取られるべきであり、且つ前記ユーザデータを暗号化するために使用されるべきであり、
前記装置が、更に、
・前記記憶媒体から前記識別された鍵データを読み取る読み取り手段と、
・前記暗号化された鍵データを解読する鍵解読手段と、
を有する、
請求項９に記載の装置。
【請求項１２】
記憶部がブロックに分かれている記憶媒体にブロックとしてユーザデータを書き込む方法であって、
・どのユーザデータが書き込まれるべきであるかを指定するユーザデータ情報と、前記ユーザデータが暗号化された形式で書き込まれるべきであるか否かを示す関連した暗号化インジケータとを含む書き込みコマンドを受信し、翻訳するステップと、
・鍵データを使用して前記ユーザデータを暗号化し、前記ユーザデータと、前記暗号化インジケータと、もし前記ユーザデーが暗号化されるならば、どの鍵データが前記ユーザデータを暗号化するために使用されるかを指定する鍵データ識別子とを書き込むステップと、
を有する方法。
【請求項１３】
選択的に暗号化された又は暗号化されない形式で記憶されるユーザデータをブロック形式で記憶し、更に、各ブロックにおいて、特に各ブロックのヘッダ又はサブヘッダにおいて、前記ブロックに記憶された前記ユーザデータが暗号化されているか否かを示す暗号化インジケータと、もし前記ユーザデータが暗号化されているならば、どの鍵データが前記ユーザデータを暗号化するために使用されたかを指定する鍵データ識別子とを記憶する記憶媒体、特に光記録可能記憶媒体。
【請求項１４】
コンピュータ上で実行される場合に、コンピュータに請求項８又は請求項１２に記載の方

法の前記ステップを実行させるコンピュータ・プログラム・コード手段を有するコンピュータ・プログラム・プロダクト。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、記憶部がブロックに分かれている記憶媒体に暗号化された形式でブロックとして記憶されるユーザデータを読み取る装置に関する。本発明は、更に、記憶媒体に暗号化された形式でユーザデータをブロックとして書き込む装置と、ユーザデータを読み取る又は書き込む対応する方法と、媒体と、コンピュータ・プログラム・プロダクトとに関する。本発明は、特に、ビデオデータ又はオーディオデータのような如何なる種類のデータでも記憶する記録可能な記憶媒体、特にＣＤ又はＤＶＤのような光記録媒体上の情報の保護に言及する。

【背景技術】

【０００２】

もしユーザデータ、例えばビデオデータ、オーディオデータ、ソフトウェア又はアプリケーションデータが記録媒体に暗号化された形式で記憶されているならば、ほとんどの場合、もし許可されるならば、認可されたアプリケーションが、インターネットのような異なる場所から解読鍵を取り出す必要なく、記録媒体から前記ユーザデータを読み取り、使用することができることが必要とされる。この故に、前記解読鍵は、前記暗号化されたユーザデータが記憶された前記媒体に記憶されなければならない。例えば無認可のアプリケーションによる、前記解読鍵に対する無認可のアクセスを防止するために、前記解読鍵は、一般に、無認可のアプリケーションが前記解読鍵を読み取ることができないように前記記憶媒体上に隠される。前記記憶媒体上に前記解読鍵を隠す既知の方法は、コンテント・スクランブリング・システム（ＣＳＳ）及び記録媒体用コンテンツ保護（ＣＰＲＭ）である。

【０００３】

一般に、記憶媒体の記憶部は、ブロック（又はセクタ）に分かれていて、ファイルの内容は、１つ以上のこのようなブロックに記憶される。読み取り又は書き込みコマンドは、一般に、論理ブロックアドレスを指定するのみであるが、読み取られるべき又は書き込まれるべきであるファイルの名前は指定しない。通常、各ブロックではなく、各ファイルが、独自の暗号化又は解読鍵を持つので、例えばＰＣアプリケーションから読み取り又は書き込みコマンドを取り出すユーザデータを読み取る又は書き込む装置は、前記読み取り又は書き込みコマンドから前記ファイルの名前を取り出さないので、解読又は暗号化のためにどの鍵データを使用するかを決定することができない。

【０００４】

１つの可能な解決法は、記憶媒体に記憶された全てのユーザデータに対して同じ鍵データを使用することだろう。しかしながら、ほとんどのアプリケーションにおいて必要とされるように、もし異なるファイルに対して異なる鍵が必要とされるならば、この解決法は許容されることができない。

【０００５】

ＤＶＤ－Ｖｉｄｅｏにおいて、各ブロックが、セクタヘッダに記憶された独自の鍵を持つ。しかしながら、前記解決法は、前記鍵のために多くの記憶容量を必要とし、従って、この記憶部は、ユーザデータのために利用されることができない。

【０００６】

他の可能な解決法は、読み取り又は書き込み装置に、どの鍵データを未来の読み取り又は書き込みコマンドにおいて使用するかを知らせるために、異なるコマンドを使用することだろう。しかしながら、幾つかのアプリケーションが同時に前記読み取り又は書き込み装置にコマンドを送信することが可能であるべきであり、各アプリケーションは、異なる鍵を使用して異なるファイルを読み取る及び／又は書き込むので、この解決法も、一般的には許容されることができない。このような解決法を用いると、単一のアプリケーションの

みが、前記読み取り又は書き込み装置にアクセスすることができるだろうが、他のアプリケーションは、同じ鍵を使用して同じファイルを読み取らない限り、除外されなければならないだろう。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

従って、本発明の目的は、上述の問題を克服するが、しかし、特に、ＰＣアプリケーションのハッキングによる窃盗に対する鍵データの高レベルの保護を提供する、ユーザデータを読み取る装置及び書き込む装置並びにユーザデータを読み取る又は書き込む対応する方法を提供することである。

【課題を解決するための手段】

【０００８】

この目的は、請求項１に記載の読み取る装置を提供することにより達成され、前記読み取る装置は、

・どのユーザデータが読み取られるべきかを指定するユーザデータ情報を含む読み取りコマンドを受信し、翻訳するコマンド・インターフェースと、

・前記記憶媒体のブロックからユーザデータ及び関連した暗号化インジケータを読み取る読み取り手段であって、前記暗号化インジケータは、前記ユーザデータが暗号化されているか否かを示し、更にもし前記暗号化インジケータが、前記ユーザデータが暗号化されていると示すならば、前記ユーザデータを解読するためにどの鍵データを使用するかを指定する関連した鍵データ識別子を読み取るように構成された当該読み取り手段と、

・前記鍵データを使用して前記ユーザデータを解読する解読手段と、

・前記解読されたユーザデータを出力する出力手段と、

を有する。

この目的は、更に、請求項７に記載のユーザデータを書き込む装置により達成され、前記書き込む装置は、

・どのユーザデータが書き込まれるべきかを指定するユーザデータ情報と、前記ユーザデータが暗号化された形式において書き込まれるべきであるか否かを示す関連した暗号化インジケータとを含む書き込みコマンドを受信し、翻訳するコマンド・インターフェースと、

・鍵データを使用して前記ユーザデータを暗号化する暗号化手段と、

・前記ユーザデータと、前記暗号化インジケータと、もし前記ユーザデータが暗号化されるならば、前記ユーザデータを暗号化するためにどの鍵データが使用されるかを指定する鍵データ識別子とを書き込む書き込み手段と、

を有する。

【０００９】

当該目的は、更に、請求項８及び請求項１２に記載の対応する方法により達成される。本発明による媒体は、請求項１３に記載される。コンピュータ上で実行される場合に、コンピュータに、請求項８又は請求項１２に記載の前記方法のステップを実行させるコンピュータ・プログラム・コード手段を有するコンピュータ・プログラム・プロダクトは、請求項１４に記載される。

【００１０】

本発明は、前記関連したユーザデータと一緒に付加的な情報を記憶し、前記ユーザデータが暗号化されているか否か、及びどの鍵データが前記ユーザデータを暗号化するために使用されたかを、前記ユーザデータを読み取る装置が認識することを可能にするというアイデアに基づく。この付加的な情報は、前記読み取る装置が、出力する前に前記ユーザデータを解読するために、関連した及び正しい鍵データを取り出すことを可能にする。同様に、ユーザデータを書き込む装置は、前記ユーザデータに加えて、前記ユーザデータが暗号化されているかを示す暗号化インジケータと、もし必要であれば、鍵データ識別子とを記憶する。前記鍵データ自身は、前記ユーザデータを最終的に受信するＰＣアプリケーショ

ンには知られないので、前記鍵データは、ハッカーによる窃盗に対して安全に保護される。加えて、ユーザデータの再暗号化は、前記ユーザデータをＰＣアプリケーションに送信する前に前記読み取る装置により実行されることができ、従って、送信中の望ましくないアクセスに対して前記ユーザデータを更に保護する。

【００１１】

好ましい実施例によると、前記鍵データ識別子は、前記鍵データ識別子により指定された前記鍵データの使用により暗号化されたユーザデータを記憶するブロックのヘッダ又はサブヘッダに記憶される。好ましくは、これは、暗号化されたユーザデータが記憶された各ブロック又はセクタにおいて行われる。加えて、前記各ブロックの前記ヘッダ又はサブヘッダに、前記暗号化インジケータが含まれる。

【００１２】

従って、たとえ前記読み取る装置が、前記ファイルの内容を解読するために使用されるべき対応する鍵データを識別することを可能にするであろうファイル名を知らないとしても、前記読み取る装置は、ブロックを読み取るときに、どの鍵が前記ブロックに記憶されたユーザデータを解読するために使用されるべきかを直ちに知る。例えばＰＣアプリケーションから、前記読み取る又は書き込む装置により受信されたコマンド、特に読み取り、再生又は書き込みコマンドは、前記ファイル名を指定しないが、アクセスされるべき前記ブロックをアドレス指定する論理ブロックアドレスと、読み取られるべき又は書き込まれるべきデータの量とを指定するのみである。

【００１３】

代替実施例によると、前記鍵データ識別子は、前記ユーザデータが読み取られるべきである前記ブロックの隣に、特にメインデータチャネルのサブチャネルに記憶される。前記鍵データ識別子は、従って、データ変調の方法で記憶されることができる。

【００１４】

もしユーザデータを暗号化するために使用された暗号化の方法が、ブロック又はセクタ間で異なり得る初期化ベクトル（ＩＶ）を組み込むならば、この初期化ベクトルも前記ブロックの前記ヘッダ又はサブヘッダの中に記憶されることが提案される。前記読み取る装置による再暗号化の場合には、このフィールドの番号が、前記ヘッダ又はサブヘッダにアクセスを持たないデータを解読する如何なるアプリケーションに対しても利用されることができるべきであるので、演繹されることができる初期化ベクトルが必要とされる。例えば、ブロック・シーケンス番号、即ちファイルを構成するブロックのシーケンスにおける特定のブロックの位置の番号が、使用されることができる。前記初期化ベクトル又は前記初期化ベクトルのために保留されるスペースは、暗号化制御情報、例えば部分的に暗号化されたブロック上の情報を含むために使用されることもできる。再暗号化されたストリームは、一定の初期化ベクトルを使用することもでき、前記一定の初期化ベクトルは、この場合、全てのデータブロックに対して同じである。

【００１５】

他の好ましい実施例によると、前記鍵データは、前記記憶媒体上に暗号化された形式で記憶され、この場合、前記鍵データは、前記ユーザデータと一緒に記憶された前記鍵データ識別子により指定されるので、前記読み取り手段により読み取られるだろう。加えて、解読手段が、前記暗号化された鍵データを解読するために設けられ、これにより前記鍵データは、前記読み取られた暗号化されたユーザデータを解読するために使用されることができる。

【００１６】

本発明の更に他の実施例によると、再暗号化は、前記記憶媒体から読み取られた前記ユーザデータを解読した後に、且つ前記ユーザデータを再暗号化された形式で出力する前に前記読み取る装置において行われる。前記読み取る装置が前記解読されたユーザデータを再暗号化することを可能にするために、再暗号化鍵データ情報は、どの再暗号化鍵データを再暗号化のために使用するかを指定する読み取りコマンドに含まれる。

【００１７】

有利に、前記鍵データ識別子は、前記記憶媒体上のアクセスされたブロックに記憶された前記ユーザデータを解読するために使用されるべきである前記鍵データを指定するのみならず、更に、前記アクセスされたブロックに記憶された前記ユーザデータに関連した付加的な情報、特に権利情報を指定し、前記付加的な情報は、前記記憶媒体上の鍵ロッカーに記憶される。前記指定された鍵データも、好ましくは、前記記憶媒体上の鍵ロッカーに含まれるルックアップテーブルに記憶される。前記鍵データ識別子は、従って、異なるブロックに対して異なる鍵データを記憶する前記ルックアップテーブルにおけるポインタとして見なされることができる。

【００１８】

特に記録可能な記憶媒体に対して、鍵データのセクタレベル記憶とファイルレベル暗号化の結合体が、加えて、本発明により、設けられてもよい。好ましくは、本発明は、ＣＤ－ＲＯＭ　ＸＡ規格を使用し、これによりこの規格との互換性が達成される。

【００１９】

本発明は、ここで図面を参照してより詳細に説明されるだろう。

【発明を実施するための最良の形態】

【００２０】

図１において、本発明による再生装置１の第１実施例が、図示される。再生装置１は、ドライブユニット２、即ち、読み取り装置と、アプリケーションを実行するアプリケーションユニット３とを有するパーソナルコンピュータ上に実施されることができる。もしユーザが、例えば、ＭＰＥＧ形式でＤＶＤに記憶されたビデオデータを再生するために、ＤＶＤ－ＲＯＭのような記録媒体４に記憶されたユーザデータを再生するつもりであれば、媒体４は、ドライブ２に挿入され、前記ユーザデータ２１及び鍵データ２２を含むデータ２０が、読み取り手段５により読み取られる。ユーザデータ２１及び鍵データ２２の両方が、媒体４に暗号化された形式で記憶され、更に、前記記録媒体に記憶する前に前記ユーザデータ及び前記鍵データを暗号化する異なる態様があるが、しかしどの特定の態様の暗号化が使用されるかは本発明に関連しないことに注目すべきである。

【００２１】

媒体４の記憶部は、論理ブロックに分かれていて、各ブロックは、論理ブロックアドレスによりアドレス指定されることができる。データがこのようなブロックの１つ以上に記憶される各ファイルは、暗号化鍵に関連するが、各ブロックは関連しない。従って、読み取り手段５は、どの暗号化鍵を媒体４から読み取られたユーザデータ２１を解読するために使用するかについて知らされる必要がある。

【００２２】

もしアプリケーションユニット３が、ドライブ２に媒体４から特定のユーザデータ２１、即ち特定のファイルを読み取るように要求するならば、コマンドユニット２４は、読み取りコマンド１９をコマンド・インターフェース６に送信する。ＳＣＳＩマルチメディア・コマンド－２（ＭＭＣ－２）又はＳＣＳＩ－３ブロック・コマンド（ＳＢＣ）に従って確立され得る読み取りコマンド１９は、これにより、媒体４から読み取る開始点を示す前記論理ブロックアドレスと、読み取られるデータの量とを含む。この情報２５は、ユーザデータ２１を含む要求されたデータ２０を読み取ることを可能にするために読み取り手段５に転送される。

【００２３】

前記論理ブロックアドレスにより示されるように媒体４上の前記ブロック又は複数のブロックにアクセスする場合、読み取り手段５は、要求されたユーザデータ２１のみならず、最初に、ユーザデータ２１が暗号化されているか否かを示す暗号化インジケータを読み取る。もしブロックのヘッダ又はサブヘッダの初めのフィールドであってもよい前記暗号化インジケータが、前記ユーザデータが暗号化されていることを示すならば、どの鍵データを前記ユーザデータを解読するために使用するかを指定する鍵データ識別子は、同じブロックの前記ヘッダ又はサブヘッダから読み取られる。前記鍵データ自身は、例えば、鍵ロッカーに含まれる目次（ＴＯＣ）において、前記記憶媒体上に暗号化された形式で記憶さ

れることができ、この場合、前記鍵ロッカーは、前記鍵データ識別子を使用して読み取り手段５によりアクセスされることができる。

【００２４】

読み取られた鍵データ２２は、読み取りの後に、読み取り手段５から供給された読み取られたユーザデータ２１を解読する解読ユニット８により要求された解読鍵ＤＫを計算する鍵計算ユニット７に入力される。解読鍵ＤＫは、媒体４に記憶する前に前記ユーザデータを暗号化するために使用された暗号化鍵と同一であるか、又はこの暗号化鍵に対応する鍵である。

【００２５】

解読の後に、解読されたユーザデータ１６は、出力手段２６によりアプリケーションユニット３に送信される。この後、前記要求されたユーザデータは、完全に再生され、レンダリングユニット１３により再生のためにレンダリングされることができる。

【００２６】

本発明によるサブヘッダの実施例は、図２に示される。ここで、ＣＤシステム内で使用するサブヘッダのサブディビジョンは、汎用ＵＤＦ（ユニバーサル・ディスク・ファイル）ファイルシステム・リーダの使用を可能にする。前記サブヘッダの最初のバイトの最初のビットは、暗号化フラグと呼ばれ、例えば、前記暗号化インジケータとして使用される。もしこのフラグが設定されれば、前記セクタの内容は暗号化され、バイト１６の残りと、完全なバイト１７は、本発明による前記鍵データ識別子として使用される、前記暗号化鍵を識別するアセットＩＤ（Asset_ID）を記憶するために使用される。

【００２７】

バイト１８の内容は、ＣＤ－ＲＯＭ　ＸＡ規格に記述されるようなサブモードに対する異なるデータを含む。もし前記暗号化フラグが、ゼロに設定されれば、バイト１６及び１７における全てのビットは、ゼロに設定されるだろう。バイト１９は、保留され、他のデータを記憶するために使用されることができる。バイト１６ないし１９の内容は、ＣＤ－ＲＯＭ　ＸＡ規格で指定されるように、バイト２０ないし２３において繰り返される。このサブディビジョンは、ＣＤ－ＲＯＭ　ＸＡを認識するシステムに対して完全な互換性があると期待される。

【００２８】

サブヘッダの他の実施例は、図３に示される。ここで、バイト２０及び２１のみが、図２に示される前記サブヘッダと比べて異なる。これらの２つのバイトは、２バイト初期ベクトル（ＩＶ）を記憶するために使用される。このような初期ベクトルは、暗号ブロック連鎖方式と呼ばれる暗号化モードを使用することにより向上された安全性を得るために大きなブロックのデータを暗号化する場合に使用される。ここで、最初の暗号ブロックが前のブロックを持たず、前記データと無関係に選択されることができる初期ベクトルが使用される。もし前記ブロック・シーケンス番号が、初期ベクトルのために使用されるならば、２バイトの使用は、前記初期ベクトルの値が再びゼロにスイッチする１２８ＭＢまでのファイルに対して充分である。しかしながら、２キロバイト以外のセクタサイズも使用される。

【００２９】

このサブディビジョンは、ほとんど全てのＣＤ－ＲＯＭ　ＸＡを認識するシステムに対して互換性があると期待される。バイト１６ないし１９における情報が、二重には存在しないという事実は、ＣＤシステムにおいて問題を伴う。第一に、前記同じブロック要求における全てのセクタは、同じアセットＩＤ（鍵データ識別子）を持つだろう。第二に、前記ブロック・シーケンス番号は、同じ要求において前の又は次のセクタより１多い又は１少ないだろう。前記サブヘッダの内容は、常に再構築されることができ、サブヘッダにおける欠陥は、前記ファイルの新しいコピーには不在であろう。

【００３０】

前記サブヘッダの使用に対する幾つかの更に他の変更があってもよい。例えば、バイト１９は、バイト２０及び２１に加えて前記初期ベクトルのために使用されてもよい。更に、

前記セクタのバイト２２及び２３も、前記初期ベクトルのために使用されてもよい。

【００３１】

ＣＤ－ＲＯＭ　ＸＡ準拠システムにおいて、前記鍵データの識別は、通常、セクタのサブヘッダのバイト１６及び１７である前記サブヘッダにおけるファイル番号及びチャネル番号フィールドの組み合わせであることもできる。前記初期ベクトルは、符号化情報のために保留されるバイト１９内、又はもし１バイトが充分でなければ、前記ファイル番号及びチャネルバイトの複製内にあることができる。

【００３２】

再生装置１の他の実施例は、図４に示される。ここで、再暗号化は、ユーザデータをアプリケーションユニット３に出力する前にドライブユニット２内で使用される。図１に示される前記第１実施例の場合のように、媒体４から読み取られるべき前記ユーザデータについての情報は、読み取りコマンド１９に含まれる。しかしながら、解読ユニット８における計算された解読鍵ＤＫによる前記ユーザデータ２１の暗号化の後に、ここで妨害の無くなった前記ユーザデータは、規則的に変わる再暗号化鍵ＲＫを使用して再暗号化ユニット１０により再暗号化される。どの再暗号化鍵ＲＫを再暗号化するために使用するかを知るために、再暗号化鍵は、認証局１５から要求されることができるか、又はドライブユニット２により要求に応じて生成されることができる。再暗号化ユニット１０による前記ユーザデータの再暗号化の後、前記ユーザデータ（１６）は、出力ユニット２６によりアプリケーションユニット３に出力される。

【００３３】

再暗号化鍵ＲＫは、前記ユーザデータを解読するためにアプリケーションユニット３にも既知でなければならないので、ドライブユニット２とアプリケーションユニット３との間の安全な認証済みチャネル１７、１８が、確立される。これを行う１つの態様は、アプリケーションユニット３上で実行するアプリケーションを認可することであり、公開鍵が、認証局１５により認証される。前記公開鍵は、この場合、安全な認証済みチャネル１７を確立するために使用される。鍵計算ユニット９は、この場合、前記認証局の署名を照合することができる。

【００３４】

前記アプリケーションの最後の認可の後、暗号化された再暗号化鍵ＲＫ又は再暗号化鍵ＲＫに関する如何なる他のデータも、安全な認証済みチャネル１８を介して、鍵計算ユニット９からアプリケーションユニット３の鍵計算ユニット１１に送信される。鍵計算ユニット１１は、従って、解読ユニット１２が再暗号化されたユーザデータ１６を解読することができるような再暗号化鍵ＲＫを計算することができる。送信線１６、１７及び１８は、再生装置１のバスに含まれることに注意すべきである。解読ユニット１２における前記ユーザデータの解読の後、前記ユーザデータは、完全に再生され、レンダリングユニット１３により再生のためにレンダリングされることができる。

【００３５】

アプリケーションユニット３１及びドライブユニット３２、即ち、ユーザデータを書き込む装置を有する本発明による記録装置３０の第１実施例が、図５に示される。ここで、アプリケーションユニット３１の入力手段３３は、媒体４に記憶されるべきユーザデータを受信し、前記ユーザデータ４１は、暗号化及び記憶のためにドライブユニット３２に送信される。加えて、書き込みコマンド４０は、コマンドユニット３４からコマンド・インターフェース３５に送信され、媒体４上の前記ユーザデータが記憶されるべき場所を指定する。暗号化されたユーザデータ４３を書き込む開始点に対する論理ブロックアドレスを含む場所情報４５は、書き込み手段３８に転送される。

【００３６】

媒体４に記憶する前にユーザデータ４１を暗号化するために、どの鍵データを使用するかを書き込む装置３２が知ることを可能にするために、鍵データ情報４２も、書き込みコマンド４０に含まれる。鍵データ識別子を含むこの鍵データ情報４２は、媒体４から前記鍵データ識別子により示された鍵データを読み取るために読み取り手段３９に転送される。

読み取られた鍵データ４４は、この場合、暗号化ユニット３６においてユーザデータ４１を暗号化するために暗号化鍵ＥＫを生成する鍵生成手段３７に入力される。

【００３７】

最後に前記暗号化されたユーザデータを媒体４上に書き込む場合、加えて、前記ユーザデータが暗号化されていることを示す暗号化インジケータ及び鍵データ識別子４２も、前記関連したユーザデータが記憶された同じブロック又はセクタに記録される。

【００３８】

媒体４から前記所要の鍵データを読み取る代わりに、前記所要の鍵データは、書き込みコマンド４０に暗号化された形式で既に含まれていてもよい。従って、前記所要の鍵データは、コマンド・インターフェース３５から、受信されたユーザデータ４１を暗号化するための暗号化鍵ＥＫを生成する鍵生成手段３７に提供されることができる。暗号化鍵ＥＫは、暗号化する暗号化ユニット３６により直接使用されることができる妨害のなくなった状態で書き込みコマンド４０に含まれることさえも可能であってもよい。

【００３９】

本発明による保護されたコンテンツを安全に与える方法は、図６を参照してここで説明されるだろう。ここで、幾つかのレベルを有するＰＣ環境におけるシステムが示される。第１レベルは、ファイル、権利及びアセット（データ）についての情報を保持するアプリケーション層５０である。第２レベルは、仮想ファイルシステム５１と、ファイルシステム・ドライバ５２と、装置ドライバ５３とを有するファイルシステム層である。仮想ファイルシステム（ＶＦＳ）５１は、変更されることができないオペレーション・システムの不可欠な部分であると見なされなければならない。結果として、アプリケーション５０からのファイルシステム・ドライバ５２に対する如何なる要求も、仮想ファイルシステム５１を透過的に通過する必要がある。これは、アプリケーション５０と仮想ファイルシステム５１との間のインターフェースは、特定の記録担体又は規格に固有であることができず、どちらも仮想ファイルシステム５１とファイルシステム・ドライバ５２との間のインターフェースであることができないことを意味する。第３レベルは、デジタル権利管理（ＤＲＭ）システムのコアを含むドライブ５４である。このレベルは、アセット、権利及びセクタについての情報を保持する。

【００４０】

ユーザデータを読み取るために、アプリケーション５０は、最初に、目次を取り出し、前記ＤＲＭシステムに権利について問い合わせる。この後、アプリケーション５０は、読み取りのために前記アセットをロックする。ドライブ５４は、前記ユーザデータの再暗号化のために新しい再暗号化鍵を生成し、アプリケーション５０は、安全な認証済みチャネル（ＳＡＣ）を介して前記新しい再暗号化鍵を得る。ファイルデータが、アプリケーション５０により読み取られる場合、初期ベクトル（ＩＶ）情報が、ドライブ５４による解読のために必要とされる。従って、媒体５５に記憶されたローカルアセットＩＤが必要とされる。前記ローカルアセットＩＤ及び／又は前記初期ベクトルは、媒体５５におけるサブヘッダ又は隠されたチャネルに記憶される。解読の後、アプリケーション５０は、前記アセットをロック解除する。

【００４１】

再暗号化のステップを含むユーザデータを書き込む方法が、図７に示される。第一に、アプリケーション５０は、書き込むために前記アセットをロックする。従って、ドライブ５４は、前記ＳＡＣを介して解読鍵を得て、ディスク５５上の記憶のための新しい鍵を生成する。アプリケーション５０は、新しいローカルアセットＩＤを取り出す。この後、アプリケーション５０は、書き込むためにファイルを開き、前記ローカルアセットＩＤをファイルシステム・ドライバ５２に通信する。更に、前記アプリケーションは、前記ファイルデータを書き込み、これにより前記再暗号化情報を前記ＳＣＳＩ書き込みコマンドに追加する。最後に、アプリケーション５０は、前記ファイルを閉じ、前記アセットをロック解除する。

【００４２】

再暗号化せずにユーザデータを書き込む方法は、図８に示される。主要なステップは図７に図示された前記方法と同一であるが、しかしながら、再暗号化は行われず、従って、前記ユーザデータを解読するための解読鍵の生成及び使用を避ける。

【００４３】

本発明は、記憶単位、即ちセクタ又はブロックの集まりから成るエンティティ、例えばファイルに対するアクセスが、元の要求を前記記憶装置上のアドレスを配置する要求に翻訳する（ソフトウェア）層、即ちドライバにより容易化され、前記アクセスされたエンティティにおける前記要求された動作の特性又は性質が、前記エンティティが記憶される前記記憶装置により使用されることができる如何なる場合にも適用されることができる。これは、光ディスクシステム及びデジタル権利管理又は割り当てストラテジのような高度な特徴を（ドライブ内に）実施するハードディスクドライブのような記憶装置の使用を含む。

【図面の簡単な説明】

【００４４】

【図１】本発明による再生装置のブロック図を示す。

【図２】ＣＤ－ＲＯＭ　ＸＡに対するサブヘッダを示す。

【図３】ＣＤ－ＲＯＭ　ＸＡに対する他のサブヘッダを示す。

【図４】再生装置の第２実施例のブロック図を示す。

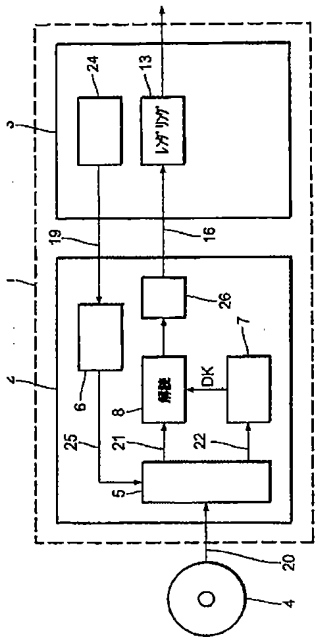
【図５】本発明による記録装置のブロック図を示す。

【図６】本発明による読み取り動作を図示する。

【図７】本発明による再暗号化を用いる書き込み動作を図示する。

【図８】本発明による再暗号化を行わない書き込み動作を図示する。

【図１】



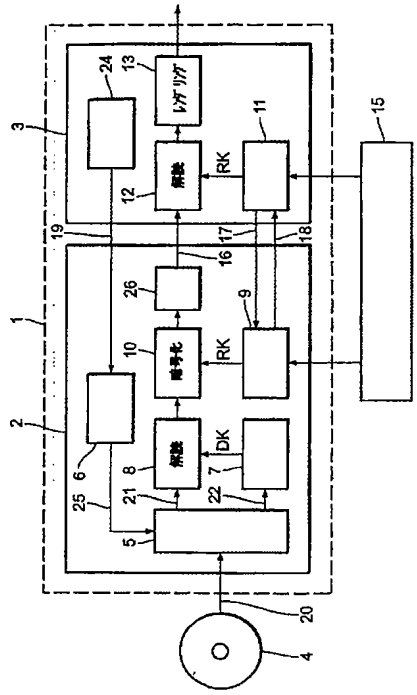
【図２】

バイト番号	ビット番号	内容	
16	0	暗号化フラグ	
	1..7	アセットＩＤ	
17	0..7		
18	0	記録の終わり	サブモード
	1	ビデオ	
	2	オーディオ	
	3	データ	
	4	トリガ	
	5	形式（0=形式１，1=形式２）	
	6	リアルタイム ブロック	
	7	ファイルの終わり	
19	0..7	保留	
20	0	暗号化フラグ	
	1..7	アセットID	
21	0..7		
22	0..7	サブモード	
23	0..7	保留	

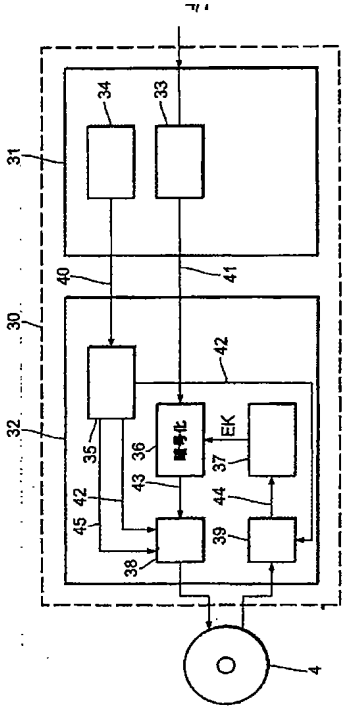
【図３】

バイト番号	ビット番号	内容
16	0	暗号化フラグ
	1..7	アセットID
17	0..7	
18	0..7	サブモード
19	0..7	保留
20		初期ベクトル
21		
22		サブモード
23		保留

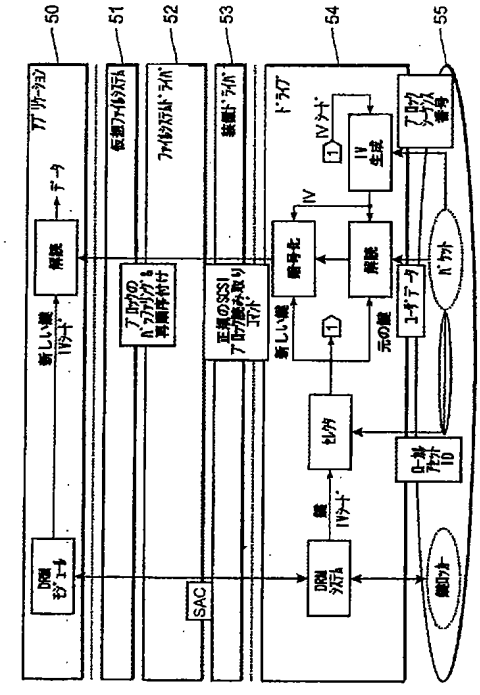
【図４】



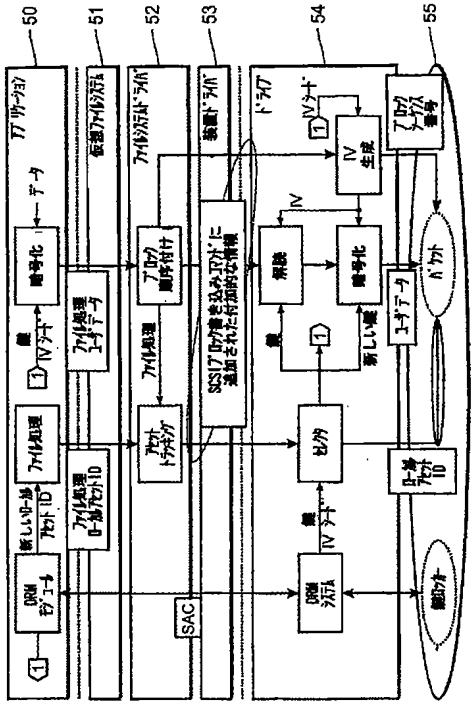
【図５】



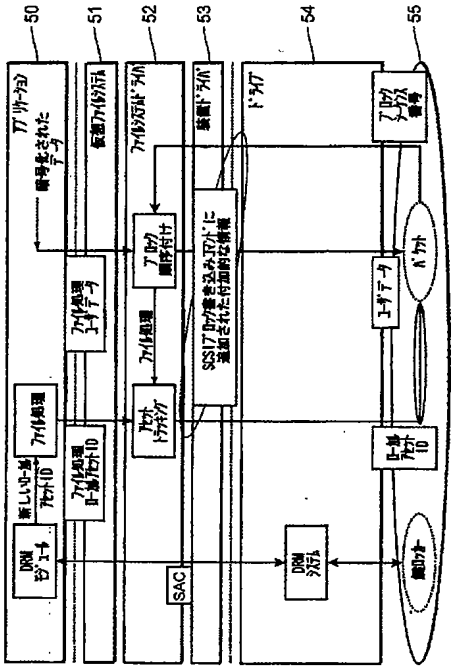
【図６】



【図７】



【図８】



【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2003 (24.04.2003)

PCT

(10) International Publication Number
WO 03/034425 A1

(51) International Patent Classification⁷: G11B 20/00, G06F 1/00

(21) International Application Number: PCT/IB02/03786

(22) International Filing Date:
12 September 2002 (12.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
01203907.9 12 October 2001 (12.10.2001) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: FONTIJN, Wilhelmus, F., J.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). STARING, Antonius, A., M.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). SENTSYN, Alexandre; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: DEGUELLE, Wilhelmus, H., G.; International Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

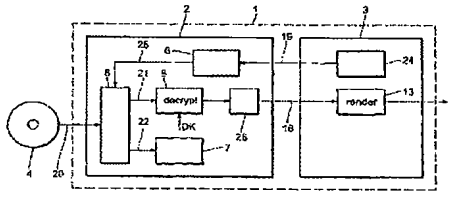
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS AND METHOD FOR READING OR WRITING BLOCK-WISE STORED USER DATA



(57) Abstract: The invention relates to an apparatus for reading or writing user data (21) stored block-wise in encrypted form on a storage medium (4), the storage of which is divided into blocks, to an apparatus (1) for writing user data (21) block-wise in encrypted form onto a storage medium (4) and to corresponding methods. Since the user data is stored on the storage medium (4) in encrypted form, the apparatus needs to be informed about the encryption key for encrypting the user data before writing it on the storage medium or about the decryption key for decryption of the read user data before outputting it. It is thus proposed according to the present invention that the apparatus for reading comprises: * a command interface (6) for receiving and interpreting a read command (19), said read command including a user data information specifying which user data are to be read, * reading means for reading user data and a related encryption indicator from a block of said storage medium, said encryption indicator indicating if said user data is encrypted or not, said reading means being further adapted for reading a related key data identifier specifying which key data (22) to use for decrypting said user data if said encryption indicator indicates that said user data are encrypted, * decryption means (7, 8, DK) for decrypting said user data using said key data, and * output means (26) for outputting said decrypted user data (16).

WO 03/034425 A1

APPARATUS AND METHOD FOR READING OR WRITING BLOCK-WISE STORED USER DATA

The invention relates to an apparatus for reading user data stored block-wise in encrypted form on a storage medium, the storage of which is divided into blocks. The invention relates further to an apparatus for writing user data block-wise in encrypted form onto a storage medium, to corresponding methods of reading or writing user data, to a medium and to a computer program product. The invention refers particularly to the protection of information on recordable storage media, particularly optical recording media like a CD or a DVD for storing any kind of data like video data or audio data.

If user data, e. g. video data, audio data, software or application data, is stored on a recording medium in encrypted form, it is most often required that an authorized application can read and use said user data, if allowed, from recording medium without the need to retrieve the decryption key from a separate location such as the internet. Hence, the decryption key has to be stored on the medium, on which the encrypted user data is stored. In order to prevent unauthorized access to the decryption key, e. g. by unauthorized applications, the decryption key is generally hidden on the storage medium such that unauthorized applications cannot read the decryption key. Known methods for hiding the decryption key on the storage medium are the Content Scrambling System (CSS) and Content Protection for Recordable Media (CPRM).

Generally, the storage of a storage medium is divided into blocks (or sectors), and the content of a file is stored in one or more of such blocks. A read or a write command generally only specifies a logical block address, but not the name of the file that shall be read or written. Since usually each file, but not each block, has its own encryption or decryption key, an apparatus for reading or writing user data that receives a read or write command, e. g. from a PC application, cannot determine which key data to use for decryption or encryption since it does not receive the name of the file from the read or write command.

One possible solution would be to use the same key data for all user data stored on a storage medium. However, this solution is not acceptable if different keys are required for different files, as is needed in most applications.

In DVD-Video each block has its own key, stored in the sector header. However, said solution requires a lot of storage capacity for the keys which storage is thus not available for user data.

Another possible solution would be to use a separate command to inform the reading or writing apparatus which key data to use in future read or write commands. However, this solution is also not acceptable in general, because it shall be possible for several applications to send commands to the reading or writing apparatus concurrently, each application reading and/or writing different files using different keys. With such a solution only a single application would be able to access the reading or writing apparatus, but other applications would have to be excluded unless they read the same file using the same key.

It is therefore an object of the present invention to provide an apparatus for reading and an apparatus for writing user data as well as corresponding methods of reading or writing user data which overcome the above mentioned problems but provide a high level of protection, in particular of the key data, against theft through hacking of a PC application.

This object is achieved by providing an apparatus for reading as claimed in claim 1, comprising:

- a command interface for receiving and interpreting a read command, said read command including a user data information specifying which user data are to be read,
- reading means for reading user data and a related encryption indicator from a block of said storage medium, said encryption indicator indicating if said user data is encrypted or not, said reading means being further adapted for reading a related key data identifier specifying which key data to use for decrypting said user data if said encryption indicator indicates that said user data are encrypted,
- decryption means for decrypting said user data using said key data, and
- output means for outputting said decrypted user data.

This object is further achieved by an apparatus for writing user data as claimed in claim 7, comprising:

- a command interface for receiving and interpreting a write command, said write command including a user data information specifying which user data are to be written and a related encryption indicator indicating if said user data shall be written in encrypted form or not,
- encryption means for encrypting said user data using key data and

- writing means for writing said user data, said encryption indicator and, if said user data are encrypted, a key data identifier specifying which key data are used for encrypting said user data.

The object is still further achieved by corresponding methods as claimed in claim 8 and claim 12. A medium according to the invention is claimed in claim 13. A computer program product comprising computer program code means for causing a computer to perform the steps of the method as claimed in claim 8 or claim 12 when said computer program is run on a computer is claimed in claim 14.

The present invention is based on the idea to store extra information together with the related user data allowing the apparatus for reading said user data to recognize if said user data are encrypted or not and which key data have been used for encrypting said user data. This extra information allows the apparatus for reading to retrieve the related and correct key data for decrypting said user data before outputting it. Similarly, an apparatus for writing user data stores, in addition to the user data, an encryption indicator indicating if said user data are encrypted and, if required, a key data identifier. Since the key data itself are not known to a PC application finally receiving the user data, said key data are securely protected against theft by a hacker. In addition, re-encryption of user data can be implemented by the apparatus for reading before transmitting it to a PC application, thus further protecting the user data against unwanted access during transmission.

According to a preferred embodiment the key data identifier is stored in the header or sub-header of a block storing user data encrypted by use of the key data specified by said key data identifier. Preferably this is done in each block or sector in which encrypted user data is stored. In addition in the header or sub-header of each block said encryption indicator is included.

Thus, even if the apparatus for reading does not know the file name which would allow it to identify the corresponding key data to be used for decrypting the content of said file, the apparatus for reading immediately knows, when reading a block, which key data are to be used for decrypting the user data stored in said block. This is particularly important since commands received by the apparatus for reading or writing, e. g. from a PC application, particularly a read, play or write command, does not specify the file name, but only the logical block address addressing the block to be accessed and the amount of data to be read or written.

According to an alternative embodiment the key data identifier is stored next to the block the user data of which are to be read, in particular in a sub-channel of a main data channel. The key data identifier may thus be stored in the method of data modulation.

If the method of encryption used for encrypting user data incorporates an initialization vector (IV), which may vary between blocks or sectors, it is proposed to store this initialization vector inside the header or sub-header of the block also. In case of re-encryption by the apparatus for reading a deducible initialization vector is needed as the number in this field should also be available to any application decrypting the data that does not have access to the header or sub-header. For instance, the block sequence number, i. e. the number of the position of a particular block in the sequence of blocks constituting a file, could be used. The initialization vector or the space reserved for the initialization vector can also be used to contain encryption control information, e. g. information on partially encrypted blocks. The re-encrypted stream could also use a constant initialization vector, which then is the same for all data blocks.

According to another preferred embodiment the key data are stored in encrypted form on the storage medium which will then be read by the reading means since they are specified by the key data identifier stored together with the user data. In addition, decryption means are provided for decrypting the encrypted key data so that they can be used for decrypting the read decrypted user data.

According to still another embodiment of the invention re-encryption is done in the apparatus for reading after decrypting the user data read from the storage medium and before outputting the user data in re-encrypted form. In order to enable the apparatus for reading to re-encrypt the decrypted user data a re-encryption key data information is included in a read command specifying which re-encryption key data to use for re-encryption.

Advantageously the key data identifier does not only specify the key data which are to be used for decrypting the user data stored in the accessed block on the storage medium, but further specifies additional information, in particular rights information, associated with the user data stored in the accessed block, said additional information being stored in a key locker on said storage medium. Also the specified key data is preferably stored in a look-up table contained in the key locker on the storage medium. The key data identifier can thus be regarded as pointer into said look-up table storing different key data for different blocks.

Particularly for recordable storage media a combination of sector level storage of key data and a file level encryption may in addition be provided according to the

invention. Preferably the invention uses the CD-ROM XA specification such that compatibility with this specification is achieved.

The invention will now be explained in more detail with reference to the drawings, in which

Figure 1 shows a block diagram of a reproducing apparatus according to the invention,

Figure 2 shows a sub-header for CD-ROM XA,

Figure 3 shows another sub-header for CD-ROM XA,

Figure 4 shows a block diagram of a second embodiment of a reproducing apparatus,

Figure 5 shows a block diagram of a recording apparatus according to the invention,

Figure 6 illustrates the read operation according to the invention,

Figure 7 illustrates the write operation with re-encryption according to the invention and

Figure 8 illustrates the write operation without re-encryption according to the invention.

In Figure 1 a first embodiment of a reproducing apparatus 1 according to the invention is illustrated. The reproducing apparatus 1 may be implemented on a personal computer comprising a drive unit 2, i. e. a reading apparatus, and an application unit 3 for running an application. If a user intends to reproduce user data stored on a recording medium 4 like a DVD-ROM, e. g. in order to replay video data stored on a DVD in MPEG-format, the medium 4 is inserted into the drive 2 where data 20 including said user data 21 and key data 22 are read by reading means 5. It should be noted that both the user data 21 and the key data 22 are stored on the medium 4 in encrypted form, and further, that there are different ways of encrypting user data and key data before storing it on the recording medium, but that it is not relevant for the present invention which particular way of encryption is used.

The storage of the medium 4 is divided into logical blocks each being addressable by a logical block address. Each file, the data of which are stored in one or more of such blocks, is associated with an encryption key, but not each block. Thus, the reading

means 5 need to be informed about which encryption key to use for decrypting the user data 21 read from the medium 4.

If the application unit 3 requests the drive 2 to read certain user data 21, i. e. a certain file, from the medium 4 a command unit 24 sends a read command 19 to the command interface 6. The read command 19 which may be established in conformity with the SCSI Multi Media Commands-2 (MMC-2) or the SCSI-3 Block Commands (SBC) thereby includes the logical block address indicating the start of reading from the medium 4 and the amount of data to be read. This information 25 is forwarded to the reading means 5 for enabling it to read the requested data 20 including the user data 21.

When accessing the block or blocks on the medium 4 as indicated by the logical block address the reading means 5 do not only read the requested user data 21 but also, at first, an encryption indicator indicating if said user data 21 is encrypted or not. If said encryption indicator, which may be the first field of a header or sub-header of a block, indicates that the user data is encrypted a key data identifier specifying which key data to use for decrypting said user data is read from the header or sub-header of the same block. The key data itself can be stored in encrypted form on the storage medium, e. g. in a table of content (TOC) contained in a key locker, which can then be accessed by the reading means 5 using said key data identifier.

The read key data 22 are after reading inputted into a key calculation unit 7 for calculating the decryption key DK required by the decryption unit 8 for decrypting the read user data 21 provided from the reading means 5. The decryption key DK is identical to an encryption key which has been used for encrypting the user data before storing it on the medium 4 or is a corresponding key to this encryption key.

After decryption the decrypted user data 16 is transmitted to the application unit 3 by output means 26. Thereafter the requested user data can be completely reproduced and rendered for playback by render unit 13.

An embodiment of a sub-header according to the invention is shown in Figure 2. Therein a sub-division of the sub-header for use within a CD system enabling the use of a generic UDF (Universal Disc File) file system reader. The first bit of the first byte of the sub-header is called the encryption flag, e. g. is used as the encryption indicator. If this flag is set the content of the sector is encrypted and the remainder of byte 16 and the complete byte 17 is used to store the Asset_ID that identifies the encryption key, i. e. which is used as the key data identifier according to the invention.

The content of byte 18 includes different data for the sub-mode as described in the CD-ROM XA specification. If the encryption flag is set to zero all bits in bytes 16 and 17 shall be set to zero. Byte 19 is reserved and could be used to store other data. The content of bytes 16 to 19 is repeated in bytes 20 to 23 as specified in the CD-ROM XA specification. This sub-division is expected to be fully compatible with CD-ROM XA aware systems.

Another embodiment of a sub-header is shown in Figure 3. Therein only bytes 20 and 21 differ compared to the sub-header shown in Figure 2. These two bytes are used to store a two byte initial vector (IV). Such initial vectors are used when encrypting a large block of data in order to obtain improved security by employing an encryption mode called cipher block chaining. Therein the first cipher block having no preceding block an initial vector is used which can be chosen independently of the data. If the block sequence number is used for an initial vector the use of two bytes would suffice for files up to 128 MB before the value of the initial vector switches to zero again. However, other sector sizes than two kilobytes are also be used.

This sub-division is expected to be compatible with almost every CD-ROM XA aware system. The fact that the information in bytes 16 to 19 is no longer present in duplicate may not involve a problem in CD systems. First, all sectors in the same block request will have the same asset_ID (key data identifier). Second, the block sequence number will be one more or one less than the previous or next sector in the same request. The content of the sub-header can always be reconstructed and a defect in a sub-header will be absent in a new copy of the file.

There may be several further variations for use of the sub-header. For instance, byte 19 may be used for the initial vector in addition to bytes 20 and 21. Still further, bytes 22 and 23 of the sector may also be used for the initial vector.

In a CD-ROM XA compliant system the identification of the key data could also be the combination of the file number and channel number fields in the sub-header which are usually bytes 16 and 17 of the sub-header of a sector. The initial vector could be in the byte 19, reserved for coding information or, if one byte is not enough, in the repetition of the file number and channel byte.

Another embodiment of a reproducing apparatus 1 is shown in Figure 4. Therein re-encryption is used within the drive unit 2 before outputting user data to the application unit 3. As in the first embodiment shown in Figure 1 an information as to the user data to be read from the medium 4 is included in the read command 19. However, after decryption of the user data 21 by the calculated decryption key DK in the decryption unit 8

the user data, now being in the clear, are re-encrypted by a re-encryption unit 10 using a regularly changing re-encryption key RK. In order to know which re-encryption key RK to use for re-encryption a re-encryption key can be requested from a certification authority 15 or generated on demand by the drive unit 2. After re-encryption of the user data by re-encryption unit 10 it (16) is outputted by the output unit 26 to the application unit 3.

Since the re-encryption key RK has also to be known to the application unit 3 in order to decrypt the user data therein, a secure authenticated channel 17, 18 between the drive unit 2 and the application unit 3 is established. One way to do this is to authorize the application running on the application unit 3 its public key is certified by a certification authority 15. Said public key is then used to establish the secure authenticated channel 17. The key calculation unit 9 may then verify the certification authority's signature.

After final authorization of the application the encrypted re-encryption key RK or any other data relating to the re-encryption key RK are transmitted from the key calculation unit 9 to the key calculation unit 11 of the application unit 3 via the secure authenticated channel 18. The key calculation unit 11 is thus able to calculate the re-encryption key RK such that the decryption unit 12 can decrypt the re-encrypted user data 16. It should be noted that the transmission lines 16, 17 and 18 are included in the bus of the reproducing apparatus 1. After decrypting the user data in decryption unit 12 it can be completely reproduced and rendered for playback by render unit 13.

A first embodiment of a reproducing apparatus 30 according to the invention comprising an application unit 31 and a drive unit 32, i. e. an apparatus for writing user data, is shown in Figure 5. Therein an input means 33 of the application unit 31 receives user data to be stored on the medium 4, which user data 41 are transmitted to the drive unit 32 for encryption and storage. In addition, a write command 40 is transmitted from the command unit 34 to the command interface 35 specifying where said user data are to be stored on the medium 4. The location information 45 including the logical block address for the start of writing the encrypted user data 43 is forwarded to the writing means 38.

In order to enable the apparatus for writing 32 to know which key data to use for encrypting the user data 41 before storing it on the medium 4 a key data information 42 is also included in the write command 40. This key data information 42 including a key data identifier is forwarded to reading means 39 for reading the key data indicated by said key data identifier from the medium 4. The read key data 44 are then inputted into the key generation means 37 generating the encryption key EK for encrypting the user data 41 in encryption unit 36.

When finally writing the encrypted user data onto the medium 4, in addition an encryption indicator indicating that said user data are encrypted and the key data identifier 42 are also recorded in the same block or sector in which the related user data are stored.

Instead of reading the required key data from the medium 4 it may also already be included in the write command 40 in encrypted form. It can thus be provided from the command interface 35 to the key generation means 37 generating the encryption key EK for encrypting the received user data 41. It may even be possible that the encryption key EK is included in the write command 40 in the clear which can directly be used by the encryption unit 36 for encryption.

The method of securely rendering protected content according to the invention shall now be explained with reference to Figure 6. Therein a system in a PC environment comprising several levels is shown. The first level is the application layer 50 which holds information on files, rights and assets (data). The second level is the file system layer comprising a virtual file system 51, a file system driver 52 and a device driver 53. The virtual file system (VFS) 51 must be considered to be an integral part of the operation system that cannot be changed. As a result any request from the application 50 to the file system driver 52 needs to pass the virtual file system 51 transparently. This means that the interface between an application 50 and the virtual file system 51 cannot be specific to a certain record carrier or standard, and neither can be the interface between the virtual file system 51 and the file system driver 52. The third level is the drive 54 containing the core of the Digital Rights Management (DRM) system. This level holds information on assets, rights and sectors.

In order to read user data the application 50 first retrieves a table of content and queries the DRM system for rights. Thereafter the application 50 locks the asset for reading. The drive 54 generates a new re-encryption key for re-encryption of the user data and the application 50 obtains the new re-encryption key via a secure authenticated channel (SAC). When file data are read by the application 50 an initial vector (IV) info is required for decryption by the drive 54. Therefore a local asset ID stored on the medium 55 is required. Said local asset ID and/or said initial vector are stored in a sub-header or hidden channel on the medium 55. After decryption the application 50 unlocks the asset.

The method of writing user data including a step of re-encryption is shown in Figure 7. At first the application 50 locks the asset for writing. Therefore the drive 54 obtains a decryption key via the SAC and generates a new key for storage on the disc 55. The application 50 retrieves a new local asset ID. Thereafter the application 50 opens the file for writing and communicates the local asset ID to the file system driver 52. Still further the

application writes the file data thereby appending the re-encryption information to the SCSI write command. Finally the application 50 closes the file and unlocks the asset.

The method of writing user data without re-encryption is shown in Figure 8. The main steps are identical to the method as illustrated in Figure 7, however no re-encryption is done, thus avoiding the generation and use of a decryption key for decrypting the user data.

The invention can be applied in any case where access to an entity, e. g. file, comprised of a collection of storage units, i. e. sectors or blocks, is facilitated by (software) layers, i. e. drivers, that translate the original request into a request for arrange of addresses on the storage device and where the properties of or the nature of the requested operation on the accessed entity can be used by the storage device the entity is stored on. This includes the use of storage devices such as optical disc systems and hard disc drives that implement (in the drive) advanced features such as digital rights management or allocation strategies.

CLAIMS:

1. Apparatus for reading user data stored block-wise on a storage medium, the storage of which is divided into blocks, comprising:

- a command interface for receiving and interpreting a read command, said read command including a user data information specifying which user data are to be read,
- reading means for reading user data and a related encryption indicator from a block of said storage medium, said encryption indicator indicating if said user data is encrypted or not, said reading means being further adapted for reading a related key data identifier specifying which key data to use for decrypting said user data if said encryption indicator indicates that said user data are encrypted,
- decryption means for decrypting said user data using said key data, and
- output means for outputting said decrypted user data.

2. Apparatus according to claim 1,

wherein said key data are stored in encrypted form on said storage medium,

wherein said reading means are adapted for reading said key data to be used for decrypting said user data, and

wherein said decryption means are further adapted for decrypting said encrypted key data.

3. Apparatus according to claim 1,

wherein said read command includes a re-encryption key data information specifying which re-encryption key data to use for re-encrypting said decrypted user data before outputting it, and

wherein said apparatus further comprises re-encryption means for re-encrypting said decrypted user data before outputting it by said output means.

4. Apparatus according to claim 1, wherein said key data identifier is stored in the header or sub-header of a block storing user data encrypted by use of the key data specified by said key data identifier.

5. Apparatus according to claim 1, wherein said key data identifier is stored next to the block the user data of which are to be read, in particular in a sub-channel of a main data channel.

6. Apparatus according to claim 1, wherein an initialization vector is stored in the header of sub-header of a block storing related user data in encrypted form.

7. Apparatus according to claim 1, wherein said key data identifier further specifies additional information, in particular rights information, associated with the user data stored in the accessed block, said additional information being stored in a key locker on said storage medium.

8. Method of reading user data stored block-wise on a storage medium, the storage of which is divided into blocks, comprising the steps of:

- a command interface for receiving and interpreting a read command, said read command including a user data information specifying which user data are to be read,
- reading means for reading user data and a related encryption indicator from a block of said storage medium, said encryption indicator indicating if said user data is encrypted or not, said reading means being further adapted for reading a related key data identifier specifying which key data to use for decrypting said user data if said encryption indicator indicates that said user data are encrypted,
- decryption means for decrypting said user data using said key data, and
- output means for outputting said decrypted user data.

9. Apparatus for writing user data block-wise onto a storage medium, the storage of which is divided into blocks, comprising:

- a command interface for receiving and interpreting a write command, said write command including a user data information specifying which user data are to be written and a related encryption indicator indicating if said user data shall be written in encrypted form or not,
- encryption means for encrypting said user data using key data, and
- writing means for writing said user data, said encryption indicator and, if said user data are encrypted, a key data identifier specifying which key data are used for encrypting said user data.

10. Apparatus according to claim 9,
wherein said write command includes the key data to be used for encrypting said user data, said key data being included in encrypted form, and
wherein said apparatus further comprises key decryption means for decrypting said encrypted key data.

11. Apparatus according to claim 9,
wherein said key data are stored in encrypted form on said storage medium,
wherein said write command includes a key data identifier identifying the key data to be read from said storage medium and to be used for encrypting said user data,
wherein said apparatus further comprises:

- reading means for reading said identified key data from said storage medium, and
- key decryption means for decrypting said encrypted key data.

12. Method of writing user data block-wise onto a storage medium, the storage of which is divided into blocks, comprising the steps of:

- receiving and interpreting a write command, said write command including a user data information specifying which user data are to be written and a related encryption indicator indicating if said user data shall be written in encrypted form or not,
- encrypting said user data using key data and writing said user data, said encryption indicator and, if said user data are encrypted, a key data identifier specifying which key data are used for encrypting said user data.

13. Storage medium, in particular optical recordable storage medium storing user data in blocks, said user data being selectively stored in encrypted or unencrypted form, further storing in each block, particularly in the header or subheader of each block, an encryption indicator indicating if said user data stored in said block is encrypted or not and a key data identifier specifying which key data are used for encrypting said user data if said user data is encrypted.

14. Computer program product comprising computer program code means for causing a computer to perform the steps of the method as claimed in claim 8 or claim 12 when said computer program is run on a computer.

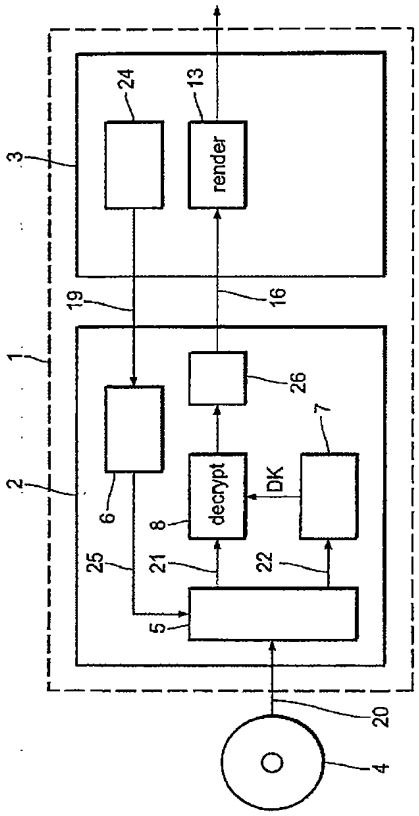


FIG.1

Byte Number	Bit Number	Content	
16	0	Encryption_Flag	
	1..7	Asset_ID	
17	0..7		
18	0	End-of-Record	Submode
	1	Video	
	2	Audio	
	3	Data	
	4	Trigger	
	5	Form (0 = Form 1, 1 = Form 2)	
	6	Real-time block	
	7	End-of-File	
19	0..7	Reserved	
20	0	Encryption_Flag	
	1..7	Asset_ID	
21	0..7		
22	0..7	Submode	
23	0..7	Reserved	

FIG.2

Byte Number	Bit Number	Content
16	0	Encryption_Flag
	1..7	Asset_ID
17	0..7	
18	0..7	Submode
19	0..7	Reserved
20		Initial Vector
21		
22		Submode
23		Reserved

FIG.3

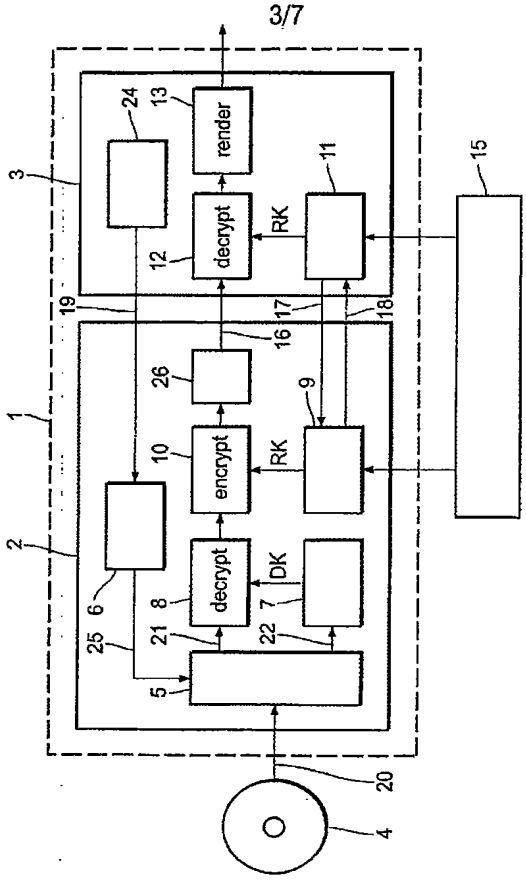

render
decrypt
RK
encrypt
RK
decrypt
DK
1
2
3
4
5
6
7
8
9
10
11
12
13
15
16
17
18
19
20
21
22
24
25
26

FIG.4

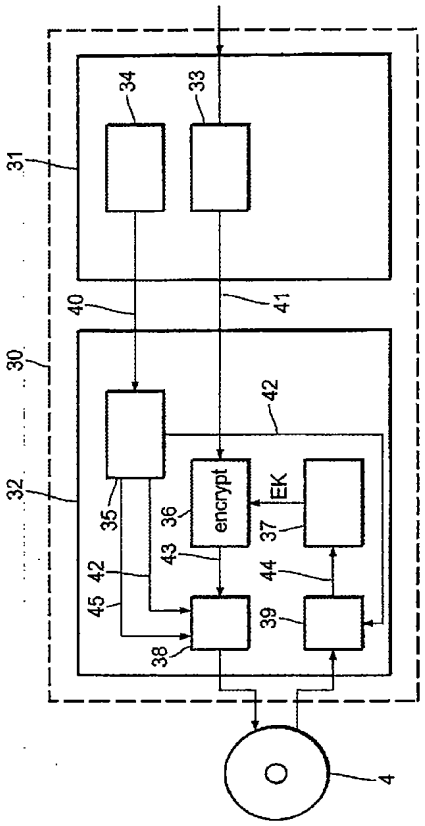


FIG.5

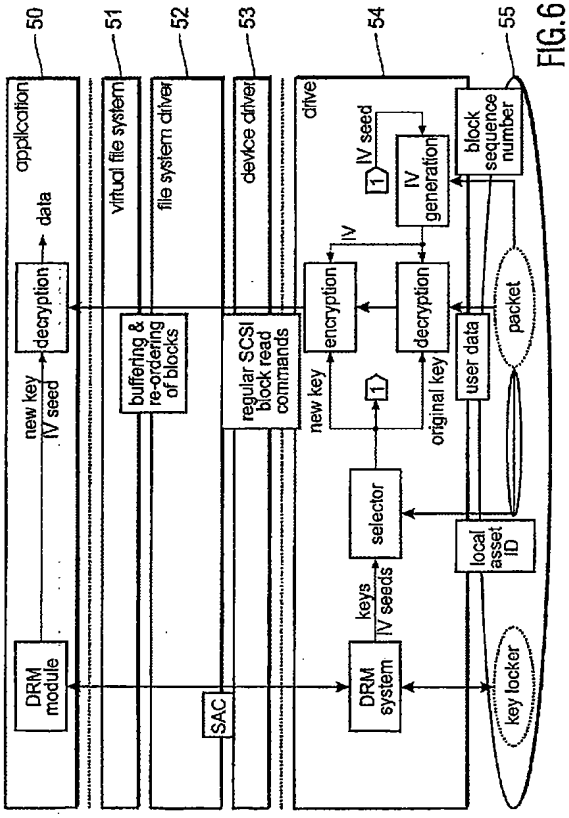

50
51
52
53
54
55
application
data
decryption
new key
IV seed
DRM module
virtual file system
buffering & re-ordering of blocks
file system driver
SAC
device driver
regular SCSI block read commands
drive
encryption
new key
IV
IV seed
IV generation
decryption
original key
selector
keys
IV seeds
DRM system
block sequence number
user data
packet
local asset ID
key locker

FIG.6

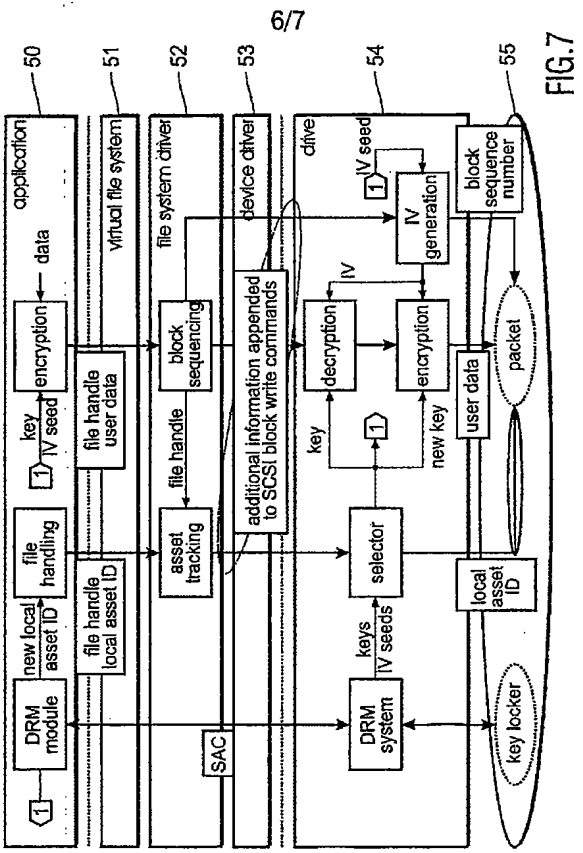

50
51
52
53
54
55
application
data
virtual file system
file system driver
device driver
drive
encryption
key
IV seed
file handle
user data
block sequencing
file handle
asset tracking
additional information appended to SCSI block write commands
file handling
new local asset ID
file handle
local asset ID
DRM module
SAC
DRM system
keys
IV seeds
selector
key
decryption
IV
IV seed
IV generation
encryption
new key
block sequence number
user data
packet
local asset ID
key locker

FIG.7

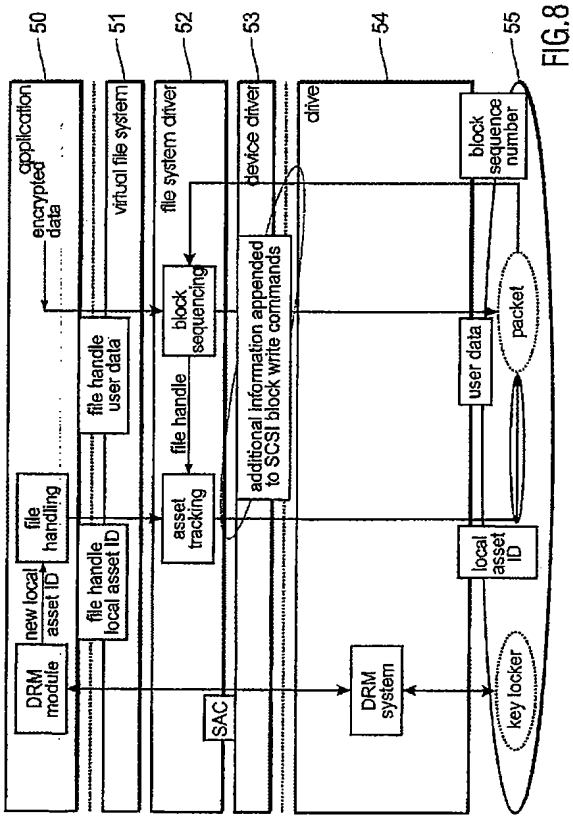

50
51
52
53
54
55
application
encrypted data
virtual file system
file system driver
device driver
drive
block sequence number
block sequencing
additional information appended to SCSI block write commands
packet
file handle user data
user data
file handle
file handling
asset tracking
local asset ID
file handle local asset ID
new local asset ID
DRM module
SAC
DRM system
key locker

FIG.8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int nal Application No
PCT/IB 02/03786

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 052 850 A (HITACHI LTD) 15 November 2000 (2000-11-15) column 6, line 33 -column 8, line 42 column 10, line 1 - line 38 figures 6,7,12,13	1-14
Y	WO 00 55861 A (IJDENS PIETER B ;TOL RONALD M (NL); JOCHEMSEN ROBERT (NL); KONINKL) 21 September 2000 (2000-09-21) page 5, line 29 -page 6, line 18 page 7, line 10 -page 8, line 33 figures 5-6B	1-14
	-/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 December 2002	07/01/2003
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Schiwy-Rausch, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inv ional Application No
PCT/IB 02/03786

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	PATENT ABSTRACTS OF JAPAN vol. 2000, no. 21, 3 August 2001 (2001-08-03) & JP 2001 103444 A (MATSUSHITA ELECTRIC IND CO LTD), 13 April 2001 (2001-04-13) abstract	1,8,9, 12,13
A	EP 1 081 888 A (MATSUSHITA ELECTRONICS CORP ;TOKYO SHIBAURA ELECTRIC CO (JP)) 7 March 2001 (2001-03-07) page 1, line 19 -page 3, line 26 claims 1-10	1,8,9, 12,13
A	PATENT ABSTRACTS OF JAPAN vol. 1997, no. 06, 30 June 1997 (1997-06-30) & JP 09 045008 A (SONY CORP), 14 February 1997 (1997-02-14) abstract	1,8,9, 12,13
A	WO 01 55858 A (ISHIBASHI YOSHIHITO ;SONY COMP ENTERTAINMENT INC (JP); AKISHITA TO) 2 August 2001 (2001-08-02)	1-4,7-14
P,A	& EP 1 195 684 A (SONY COMP ENTERTAINMENT INC (JP);SONY CORP (JP)) 10 April 2002 (2002-04-10) column 19, line 25 -column 24, line 8 column 85, line 50 -column 88, line 33 figures 4-6,53-55	1-4,7-14
A	EP 0 951 019 A (HITACHI LTD) 20 October 1999 (1999-10-20) column 1, line 32 -column 2, line 25 column 3, line 10 -column 5, line 33 column 9, line 47 -column 10, line 17 column 11, line 51 -column 12, line 2	1,8,9, 12,13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/03786

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1052850	A	15-11-2000	JP 2000322825 A		24-11-2000
			EP 1052850 A2		15-11-2000
WO 0055861	A	21-09-2000	WO 0055861 A1		21-09-2000
			WO 0055736 A1		21-09-2000
			EP 1076857 A1		21-02-2001
			EP 1086467 A1		28-03-2001
JP 2001103444	A	13-04-2001	NONE		
EP 1081888	A	07-03-2001	BR 0003884 A		03-04-2001
			CN 1286457 A		07-03-2001
			EP 1081888 A2		07-03-2001
			JP 2001142394 A		25-05-2001
			SG 87160 A1		19-03-2002
JP 09045008 4	A		NONE		
WO 0155858	A	02-08-2001	JP 2001209583 A		03-08-2001
			AU 2882901 A		07-08-2001
			BR 0104213 A		08-01-2002
			CN 1366637 T		28-08-2002
			EP 1195684 A1		10-04-2002
			WO 0155858 A1		02-08-2001
			NZ 513833 A		28-09-2001
			US 2002154779 A1		24-10-2002
EP 0951019	A	20-10-1999	CN 1239293 A		22-12-1999
			EP 0951019 A2		20-10-1999
			JP 2000003559 A		07-01-2000
			JP 2001236729 A		31-08-2001
			SG 72943 A1		23-05-2000
			TW 425543 B		11-03-2001

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51)Int.Cl.[7]	F I	テーマコード（参考）
	G11B 20/10 301Z	

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100122769
弁理士 笛田 秀仙
(72)発明者 フォンティン ウィルヘルムス エフ ジェイ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6
(72)発明者 スタリング アントニウス エイ エム
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6
(72)発明者 シニツィン アレクサンドレ
オランダ国 ５６５６ アーアー アインドーフェン プロフ ホルストラーン 6

Fターム(参考) 5B017 AA03 BA07
5D044 AB05 AB07 BC04 CC04 DE17 DE50 EF05 FG18 GK11 GK17
HL08
5J104 AA12 AA16 AA32 EA04 EA15 EA18 EA20 JA03 NA02 NA27
NA37 PA14

【要約の続き】
化されていることを示すならば、前記ユーザデータを解読するために、どの鍵データ（２２）を使用するかを指定する関連した鍵データ識別子を読み取るように構成された当該読み取り手段と、＊前記鍵データを使用して前記ユーザデータを解読する解読手段（７、８、ＤＫ）と、＊前記解読されたユーザデータ（１６）を出力する出力手段（２６）とを有することが提案される。